A Software Flaw Taxonomy: Aiming Tools at Security

Sam Weber, Paul A. Karger, and Amit Paradkar. *Proceedings of Software Engineering for Secure Systems – Building Trustworthy Applications (SESS'05)*, 2005.

Abstract from the first page:

Although proposals were made three decades ago to build static analysis tools to either assist software security evaluations or to find security flaws, it is only recently that static analysis and model checking technology has reached the point where such tooling has become feasible. In order to target their technology on a rational basis, it would be useful for tool-builders to have available a taxonomy of software security flaws organizing the problem space. Unfortunately, the only existing suitable taxonomies are sadly out-of-date, and do not adequately represent security flaws that are found in modern software.

In our work, we have coalesced previous efforts to categorize security problems as well as incident reports in order to create a security flaw taxonomy. We correlate this taxonomy with available information about current high-priority security threats, and make observations regarding the results. We suggest that this taxonomy is suitable for tool developers and to outline possible areas of future research.

Part "Attachment Data"

Mime-type: application/pdf, size: 130008 bytes